PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-085014
(43)Date of publication of application : 30.03.1999

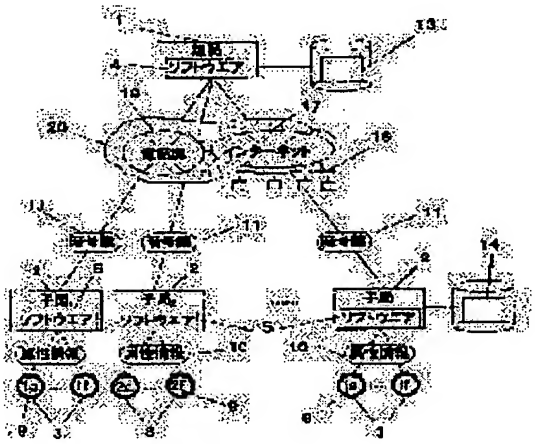
(51)Int.Cl. G09C 1/00
H04L 9/08

(21)Application number : 09-287538
(22)Date of filing : 12.09.1997

(71)Applicant : MATSUMOTO TERUO
(72)Inventor : MATSUMOTO TERUO

(54) METHOD OF EXCHANGING CIPHER INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To exchange information through an open information communication network by specifying a communication partner with security ensured.
SOLUTION: A primary station 1 generates a cryptographic key or a cryptographic key and an encipherment system 11 on a request from an application service or a user 3, and updates and manages the cryptographic key or the cryptographic key and enciphement system 11 corresponding to a user identification code 9 for the primary station cryptographic key management data 13 and distributes them to secondary stations 2. The secondary stations update and manage the cryptographic key or cryptographic key and encipherment system 11 distributed to secondary station cryptographic key management data 14 corresponding to the user identification code 9. The user 3 ciphers or deciphers the information by the cryptographic key or the cryptographic key and encipherment system 11 stored at the secondary station for transmitting and receiving the information, and uses the result of the executed application service.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

1 / 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－85014

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	FI	
G09C 1/00	630	G09C 1/00	630B
H04L 9/08		H04L 9/00	601D
			601B

審査請求　未請求　請求項の数14　書面　（全 18 頁）

(21)出願番号　特願平9－287538

(22)出願日　平成９年(1997)９月12日

(71)出願人　596070515
松本　輝夫
神奈川県平塚市日向岡２丁目６番地17号

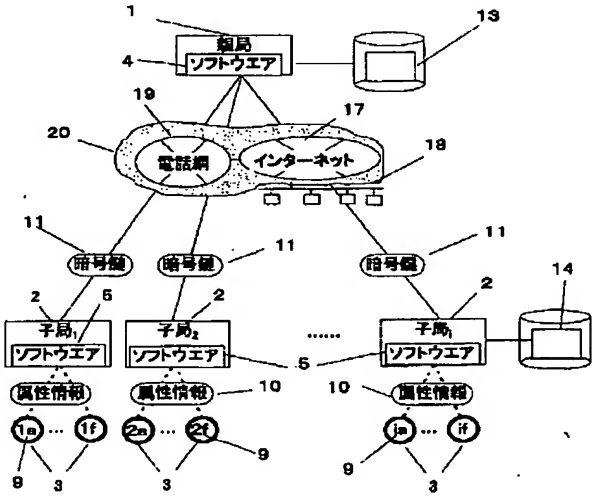
(72)発明者　松本　輝夫
神奈川県平塚市日向岡２丁目６番地17号

(54)【発明の名称】　暗号情報交換方式

(57)【要約】　（修正有）

【課題】オープンな情報通信網で通信相手を特定しセキュリティを保って情報交換を行う。

【解決手段】アプリケーションサービスもしくは利用者３の要求で親局１は暗号鍵もしくは暗号鍵と暗号方式１１を生成し、親局暗号鍵管理データ１３へ利用者識別記号９と対応して暗号鍵もしくは暗号鍵と暗号方式１１を更新管理し、子局２へ配布する。子局２は子局暗号鍵管理データ１４へ利用者識別記号９と対応して配布された暗号鍵もしくは暗号鍵と暗号方式１１を更新管理する。利用者３は子局２で格納された暗号鍵もしくは暗号鍵と暗号方式１１で情報を暗号化もしくは復号化して情報の送受信を行いアプリケーションサービスの実行結果を利用する。



【特許請求の範囲】

【請求項１】インターネット（１７）、ＬＡＮ（１８）並びに公衆電話網（１９）を含むＷＡＮ（２０）を経由して、親局（１）へ加入接続した子局（２）並びに、利用者属性情報（１０）を子局（２）を通じてもしくは直接親局（１）へ登録し、親局（１）が生成した利用者識別記号（９）を授けられた利用者（３）の三者で構成するアプリケーションサービスを実行する通信網において、アプリケーションサービスもしくは利用者（３）からの暗号鍵もしくは暗号鍵と暗号方式（１１）の配布要求で、親局（１）は利用者（３）毎の暗号鍵もしくは暗号鍵と暗号方式（１１）を生成又は選択して、利用者（３）の利用者識別記号（９）が格納されている子局（２）へ平文もしくは暗号化して配布し、親局暗号管理データ（１３）に利用者（３）毎の暗号鍵もしくは暗号鍵と暗号方式（１１）を更新管理し、子局（２）は子局暗号管理データ（１４）に利用者（３）毎の暗号鍵もしくは暗号鍵と暗号方式（１１）を更新管理し、利用者（３）は子局（２）もしくは親局（１）を通じて暗号鍵もしくは暗号鍵と暗号方式（１１）を使用して情報を暗号化もしくは復号化して他の利用者（３）もしくは親局（１）との間で情報の交信を行う暗号情報交換方式。

【請求項２】請求項１において、子局（２）が最初に親局（１）へ接続する時に、親局（１）は子局識別記号（１２）を生成し、親局暗号鍵管理データ（１３）に、子局識別記号（１２）を通して利用する利用者（３）の利用者識別記号（９）を参照できるように記録、保管管理し、子局識別記号（１２）もしくは暗号化した子局識別記号（１２）を子局（２）へ配布し、子局（２）は配布された自局の子局識別記号（１２）を子局暗号鍵管理データ（１４）に格納し、更に、利用者（３）が親局（１）へ登録する時に、親局（１）から子局（２）へ配布される利用者識別記号（９）も子局暗号鍵管理データ（１４）へ格納し、利用者（３）が子局（２）もしくは親局（１）を通してアプリケーションサービスへ参加する時、子局暗号鍵管理データ（１４）もしくは親局暗号鍵管理データ（１３）で格納されていない利用者識別記号（９）の利用者（３）はアプリケーションサービスへの参加を拒絶され、格納されている利用者識別記号（９）の利用者（３）は子局（２）もしくは親局（１）を通して、利用者識別記号（９）及び利用者属性情報（１０）と子局識別記号（１２）を一緒に親局（１）へ送信し、親局（１）は利用者（３）が子局（２）もしくは親局（１）を通してアプリケーションサービスに参加している事を確認して利用者（３）の認証を行う暗号情報交換方式。

【請求項３】請求項１もしくは請求項２に於いて、既に利用者（３）が子局（２）もしくは親局（１）を通して親局（１）に登録している場合、同じ利用者（３）が利用者識別記号（９）を格納した別の子局（２）を通してアプリケーションサービスへ参加できる暗号情報交換方式

【請求項４】請求項３に於いて、既に親局（１）へ登録の済んだ利用者（３）は利用者識別記号（９）が格納されていない子局（２）もしくは親局（１）を通じてアプリケーションサービスを利用する手続きを行い、既に利用者識別記号（９）が格納されている子局（２）を通して、認証を親局（１）に申請し、利用者（３）を認証した親局（１）は親局暗号鍵管理データ（１３）へ利用者識別記号（９）毎に子局識別記号（１２）を記録、保管管理し、利用者識別記号（９）が格納されていない子局（２）へ利用者識別記号（９）を配布し、子局（２）は子局暗号鍵管理データ（１４）へ利用者識別記号（９）を格納し、利用者（３）は新しい子局（２）もしくは親局（１）を通してアプリケーションサービスへ参加できる利用者（３）の認証を行う暗号情報交換方式。

【請求項５】請求項３に於いて、親局（１）から子局（２）へ利用者（３）毎に一度に複数個の暗号鍵もしくは暗号鍵と暗号方式（１１）を配布しておき、配布済みの複数の暗号鍵もしくは暗号鍵と暗号方式（１１）を親局（１）と子局（２）の間で鍵を更新管理する情報（１５）で親局（１）及び子局（２）の暗号鍵もしくは暗号鍵と暗号方式（１１）を更新する暗号情報交換方式

【請求項６】請求項５において、N_i 個の子局（２）を接続した親局（１）から、N_k 個の子局（２）を接続した親局（１）がＫ個だけ存在したとして、Ｋ個の親局（１）を子局（２）として接続された親局（１）を設けた事を特徴とする、階層的な暗号情報交換方式

【請求項７】請求項６に於いて、親局（１）は子局（２）に既に配布した暗号鍵もしくは暗号鍵と暗号方式（１１）で新しい暗号鍵もしくは暗号鍵と暗号方式（１１）を暗号化して子局（２）に配布し、子局（２）は既に受信している暗号鍵もしくは暗号鍵と暗号方式（１１）で、受信した暗号化された暗号鍵もしくは暗号鍵と暗号方式（１１）を復号化し、子局（２）の子局暗号鍵管理データ（１４）に格納されている暗号鍵もしくは暗号鍵と暗号方式（１１）を更新格納する暗号情報交換方式。

【請求項８】請求項６に於いて、親局（１）は新しい暗号鍵もしくは暗号鍵と暗号方式（１１）を既に子局（２）へ配布した暗号鍵もしくは暗号鍵と暗号方式（１１）を使用せず暗号化して子局（２）に配布し、子局（２）はこの暗号を復号化して子局暗号鍵管理データ（１４）に格納する暗号情報交換方式。

【請求項９】請求項７もしくは請求項８に於いて、送信元の利用者（３）が送信したい単数もしくは複数の利用者（３）宛の情報を暗号化して親局（１）に送信し、親局（１）は暗号を復号化して、送信先の利用者（３）の暗号鍵もしくは暗号鍵と暗号方式（１１）で暗号化し、送信先の利用者識別記号（９）が格納されている子局

（２）宛に送信し、送信先の利用者（３）は暗号を復号化して送信元の利用者（３）からの情報を受信し、送信元と送信先の間で親局（１）を中継して暗号情報の交信を行う暗号情報交換方式。

【請求項１０】請求項７もしくは請求項８に於いて、利用者（３）が交信したい単数もしくは複数の利用者（３）と直接交信を行う前に、親局（１）は受信元の利用者（３）の暗号鍵もしくは暗号鍵と暗号方式（１１）を送信元の利用者識別記号（９）が格納されている子局（２）へ配布し、送信元の利用者（３）は配布された暗号鍵もしくは暗号鍵と暗号方式（１１）で情報を暗号化して、送信先の利用者（３）へ直接送信し、受信した利用者（３）は暗号を復号化し情報を交信する暗号情報交換方式。

【請求項１１】請求項７もしくは請求項８に於いて、アプリケーションサービス、もしくは利用者（３）の要求で、親局（１）は限定された利用者（３）に共通の暗号鍵もしくは暗号鍵と暗号方式（１１）もしくは暗号確認情報（２３）を生成もしくは選択し、利用者（３）の利用者識別記号（９）が登録された子局（２）もしくは親局（１）へ配布し、暗号情報の交信を行う暗号情報交換方式

【請求項１２】請求項７もしくは請求項８に於いて、利用者（３）と親局（１）の間で暗号化した情報の交信を行う暗号情報交換方式。

【請求項１３】請求項９及び請求項１０及び請求項１１の情報交信方式において、アプリケーションサービスに必要な複数の利用者（３）の情報が時間的にずれて親局（１）に着信する場合、アプリケーションサービスで必要な情報が親局（１）に全て着信した後、複数の利用者（３）に関わるアプリケーションサービスの処理を親局（１）が行う暗号情報交換方式。

【請求項１４】請求項１２及び請求項１３において、暗号情報交換機能を使う子局用のアプリケーションソフトウエ（５）をインストールし、子局（２）に格納されている利用者識別記号（９）の利用者（３）が直接入力操作を行わずアプリケーションサービスが子局（２）に格納されている利用者識別記号（９）の利用者（３）に代わって、その他の利用者（３）との暗号情報を交信する暗号情報交換方式。

【発明の詳細な説明】

【０００１】

【目的】通信網として、ＬＡＮ、公衆電話網の交換接続網、インターネットは安価でオープンな通信網として世界的に拡充しつつある。インターネット及び電話網を含むＷＡＮに参加した全の人々にとってオープンで接続が容易なだけ、情報の内容を第三者が容易に覗る事ができる。従って、これらの通信網の弱点は通信網のセキュリティを如何に克服するかである。通信網上のセキュリティの問題として、予期しない相手が通信設備に侵入し、データやシステムの盗聴や破壊行為を如何にして防ぐかと言う問題やシステムやデータを破壊するウイルスから如何に身を守るかの外に、データ交信中、それらの情報を盗聴したり、交信相手が見えない通信網の性質を悪用した利用を如何に防ぐのかと言う問題がある。

【０００２】交信中に生じる問題を防ぐには、交信相手が確かに間違いない相手だと如何にして確認するかの認証の問題、及び、情報を当事者以外内容を理解できないようにする情報暗号化を行う上で、情報を暗号化する暗号鍵のやりとりを如何に安全に行うかと言う問題の２点に絞られて来る。この発明は交信している相手が正しい相手だといかにして確認するか及び、関係者だけが使用できる様に暗号鍵や暗号方式を如何にして安全にやり取りするかに関するものである。

【０００３】

【発明の属する技術分野】電子情報通信網での安全な情報交換を如何に行うかの暗号情報交換方式に関している。

【０００４】

【従来の技術】情報通信網での安全な情報交換を如何に行うか古くから研究が行われているが、近年インターネットの普及につれて、安全な情報の交信が重要になってきている。情報通信網で交信される情報の安全性を確保する為に、情報を暗号化して送信し関係者以外判読出来ないようにするための、情報を暗号化する暗号方式や、暗号鍵を安全に届けるために暗号鍵を公開鍵と秘密鍵の双方を使って本人を認証し、情報を暗号化及び復号化する方式に関する提案がなさている。又、１回限りのパスワード（１６）を発生さる方法で、本人の認証を行うなどが研究されている。

【０００５】

【発明が解決しようとする課題】オープン性の高い情報通信網での情報交信の課題は、情報交換や、商取引等での利用に対して次の様な課題がある。

１　暗号鍵配布の管理工数がかかる

２　個人が暗号鍵を記憶するリスクからの解放

３　盗聴、暗号解読に対するセキュリティの確保

４　デリバリー決済時における、決済システムのリスクの減少

５　本人の認証性の確保

【０００６】Ｎ人の間で相互に暗号鍵を配布すると、（図４）ａにおいて、Ｎ（Ｎ－１）／２の経路で暗号鍵を配布する管理工数が発生する。このコストを減少するのが一つの課題なる。

【０００７】暗号化した情報を暗号鍵で復号する為には暗号鍵を記憶していなければならない。暗号が簡単に解読されない様にするために暗号鍵が長くなり、人間が記憶する限界を超えて来る。そうなると、暗号鍵を管理するためのパスワード管理が必要になったりして、結局人間の記憶力の限界に対応した管理が要請される。ＩＣカ

ードを使って、秘密鍵を人間の記憶と切り離す等の試みも考えられるが、カードを紛失した場合の問題など、個人で管理する暗号鍵のセキュリティは必ずしも強くない。このような暗号鍵の管理は情報通信網を気軽に利用出来る機会を遠ざける。

【０００８】情報通信網での交信を盗聴されたり、暗号化していても解読されるのを如何に防ぐか大きな課題である。更に、情報が盗まれるだけなく、盗まれた情報を使用して、本人に成りすまして窃盗を働いたりされると被害を大きくする。このような被害を如何に防ぐか中心的な課題である。

【０００９】店頭販売に比較して、通信網上で商品と代金を如何に決済するかが一つの課題である。商品を配送した時に代金と引き替えに商品を渡したり、代金を先に送金した後、商品を送達したり、もしくは、商品を送達後代金を振り込んだりしている。商品の配送を伴う情報網上での商取引では代金と商品を相対決済できないと、商品又は代金を払った方がリスクを負う。情報通信網での取引にも相対取引が望ましい。

【００１０】本人を偽って窃盗を行って本人に被害を与えたり、他人の情報を盗み出したり、他人のソフト財産を破壊したりする犯罪は情報通信網で大きな問題である。通信の相手が本人か否か如何にして認証するか最大の課題である。

【００１１】

【課題を解決する為の手段】この発明の概念は、親局が必要に応じて、使い捨ての暗号鍵［Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ］もしくは使い捨ての暗号鍵と暗号方式を生成し、子局に配布するので、利用者の暗号鍵もしくは暗号鍵と暗号方式は変化してゆく、そのため、盗聴しようとしても、暗号を解読しなければならず、もしある時間を経過して暗号の解読に成功したとしても、使い捨ての暗号鍵もしくは使い捨ての暗号鍵と暗号方式が変化しているので、利用者に成りすまそうとしても、親局が配布した暗号鍵もしくは暗号鍵と暗号方式と異なっているので、利用者に成りすまそうとしている偽者の暗号を親局が復号化できず、本人と認証してくれない。

【００１２】図１及び図２で暗号情報交換機能を使う親局用のアプリケーションソフトウエア（４）をインストールし、暗号情報交換機能の親局の分担機能（６）を持ち、インターネット（１７）、ＬＡＮ（１８）、公衆電話網（１９）を含むＷＡＮ（２０）を経由して、親局（１）に加入接続した子局（２）と暗号情報の交信を行うパソコンもしくはワークステーション等の情報機器で構成される親局（１）と、暗号情報交換機能の子局の分担機能（８）を組み込んだ暗号情報交換機能を使う子局用のアプリケーションソフトウエア（５）をインストールし、親局（１）に加入接続したパソコンもしくは移動情報端末もしくはワークステーション等の情報機器で構成される子局（２）と、暗号情報交換機能の利用者（３）の分担機能（８）を持ち、親局（１）に登録された利用者（３）、もしくは子局（２）にインストールされたアプリケーションソフトウエア（５）で利用者（３）の機能を代替する子局（２）と一体化した利用者（３）から成る暗号情報交換通信網を構成する。

【００１３】親局（１）と子局（２）との間だけで暗号鍵もしくは暗号鍵と暗号方式（１１）の交信を行い、子局（２）の間で暗号鍵もしくは暗号鍵と暗号方式（１１）を直変更する様な事をしない。従って、暗号化された暗号鍵もしくは暗号鍵と暗号方式（１１）は親局（１）が一元化して管理しているので、子局（２）の間で、暗号鍵の管理に関する負荷が懸からず、暗号情報を送信途中、仮に盗聴されたとしても、暗号を解読しない限り、第三者は暗号鍵もしくは暗号鍵と暗号方式（１１）を知ることが出来ず、安全に配布できる。

【００１４】親局（１）と子局（２）及び利用者（３）の暗号情報交換に関する分担機能は図２で、暗号情報交換機能の親局の分担機能（６）は

１．利用者（３）からの暗号鍵もしくは暗号鍵と暗号方式（１１）の発行要求、もしくはアプリケーションサービスでイベントが発生した時の発行要求、あるいはランダム、もしくは一定の設定した回数毎もしくは、ランダム、もしくは一定の間隔に設定した時間毎の発行要求を受けて、親局（１）は利用者（３）毎に単数のもしくは複数の暗号鍵もしくは暗号鍵と暗号方式（１１）を生成もしくは選択する。

２．親局暗号鍵管理データ（１３）へ、利用者識別記号（９）毎に生成もしくは選択した暗号鍵もしくは暗号鍵と暗号方式（１１）を更新する。

３．利用者（３）の利用者識別記号（９）が格納されている子局（２）へ生成もしくは選択した暗号鍵もしくは暗号鍵と暗号方式（１１）を配布する。

４．利用者（３）の登録時、利用者識別記号（９）を生成し、親局暗号鍵管理データ（１３）へ記録し、利用者識別記号（９）と対応を付けて利用者属性情報（１０）を記録し、利用者（３）が子局（２）を通して親局（１）へ接続した子局（２）へ利用者識別記号（９）を配布し、親局（１）が登録を認めたことを利用者へ連絡する

５．子局（２）の加入接続時、子局識別記号（１２）を生成し、親局暗号鍵管理データ（１３）へ記録し、子局（２）へ配布する。

６．子局（２）の入力受付と子局（２）との通信制御

７．暗号情報交換方式を利用したアプリケーションサービスを実行する機能

８．暗号化された利用者識別記号（９）と利用者属性情報（１０）及び子局識別記号（１２）を受信し、親局暗号鍵管理データ（１３）と突き合わせて利用者（３）の認証を行う。

９．子局（２）との情報交信に際し、情報を暗号化し、複合化する。

【００１４】これに対応する暗号情報交換機能の子局の分担機能機能（７）は

１．親局（１）との通信制御

２．利用者識別記号（９）を格納している利用者（３）毎の暗号鍵もしくは暗号鍵と暗号方式（１１）を利用者識別記号（９）毎に更新して格納する。

３．親局（１）が子局（２）に配布した子局識別記号（１２）を格納し、子局識別記号（１２）を利用者識別記号（９）と一緒に利用者属性情報（１０）を親局（１）に送信する。

４．子局（２）は子局暗号鍵管理データ（１４）に格納している単数あるいは複数の利用者識別記号（９）を確認して、利用者識別記号（９）が格納されていない利用者（３）のアプリケーションサービスへの参加を拒絶する。

５．子局（２）は登録している利用者属性情報（１０）の一部もしくは全てを利用者（３）本人以外の第三者が見ることが出来ないように子局（２）へ格納しておき、利用者（３）が属性情報を手で入力する手間を省略する事も出来る。

６．利用者（３）からのパスワード（１６）の変更申請を受け付けて、親局（１）へ更新情報を送信し、子局（２）が内部で格納している場合は格納しているデータの変更処理を行う。

７．利用者（３）が子局（２）を通して他の子局（２）もしくは親局（１）と情報交信を行う際、格納された利用者（３）毎の暗号鍵もしくは暗号鍵と暗号方式（１１）を使って、情報を暗号化し、複合化する。

【００１５】最後に暗号情報交換機能の利用者の分担機能（８）は

１．子局（２）もしくは親局（１）を通してアプリケーションサービスで要求する利用者（３）としての属性情報（１０）を入力、送信し、アプリケーションサービスで要求している手続きを行い利用者（３）として親局（１）に登録する。

２．子局（２）もしくは親局（１）を通して、アプリケーションサービスを実行し利便をうる。

３．子局（２）を通して利用者属性情報（１０）の一部、もしくは全ての情報を利用者（３）が入力するが、属性情報の一部もしくは全てを子局（２）へ格納しておき操作性を楽に出来る。

４．アプリケーションサービスによっては暗号情報交換機能を使う子局用のアプリケーションソフトウエア（５）を子局（２）にインストールし、全て、もしくは大部分の入出力機能を利用者（３）に代わって代行し、利用者（３）の入出力操作無しで子局（２）はアプリケーションサービスが実行可能となる。一般にアプリケーションサービスを提供する側の利用者（３）は子局（２）と一体となるので、暗号情報交換機能を使う子局用のアプリケーションソフトウエア（５）が利用者（３）の機能を殆ど全て代行する。

５．利用者（３）の記憶で管理しているパスワード（１６）を随時変更する。

【００１６】利用者（３）が親局（１）に登録して、本人であることの認証を得る為に子局（２）と親局（１）の間で送受信する利用者属性情報（１０）として次の３つの分類で整理する。

１　親局（１）が生成し管理する情報

ａ　利用者識別記号（９）

ｂ　子局識別記号（１２）

２　利用者（３）の記憶で管理する情報

ａ　パスワード（１６）

３　利用者（３）の社会的な情報

ａ　氏名

ｂ　住所

ｃ　加入者電話番号

ｄ　電子メールアドレス

ｅ　免許証・保険証・戸籍抄本・印鑑証明等公に発行された本人を確認する書類に記された整理番号等

ｇ　勤務先

親局（１）が生成し管理する情報は、子局（２）及び利用者（３）が親局（１）に加入接続もしくは登録時に親局（１）が生成管理する情報で、子局の識別記号（１２）は子局（２）を親局（１）が識別するために使用するので、子局（２）のそれぞれに独自の記号を割り当てる。親局（１）だけが子局識別記号（１２）を管理し、子局（２）に配布して、親局暗号鍵管理データ（１３）及び、子局暗号鍵管理データ（１４）で子局識別記号（１２）を保管している。利用者識別記号（９）は利用者（３）に知らせて、親局（１）及び子局（２）で保管管理し、氏名に代わって利用される。利用者（３）の記憶で管理する情報としてパスワード（１６）がある。この情報は原則として、利用者（３）がアプリケーションサービスの利用に先立って、子局（２）を通じて手で入力し親局（１）が利用者（３）の認証の為の情報として利用する。パスワード（１６）は原則として、利用者（３）の記憶によってのみ保持されるが、利用性を上げるため、子局（２）の中に第三者が窺い知れないように格納する事も可能である。パスワード（１６）は第三者への漏洩を防止するために、随時、子局（２）で変更手続きを行い、親局（１）もしくは子局（２）で管理している利用者（３）毎のパスワード（１６）を変更する。利用者（３）の社会的な情報として、氏名や、住所等がある。これらの情報は、利用者（３）が最初親局（１）に登録する時に利用者（３）の確認をかねて登録する情報で、利用の度毎に、逐一、この情報を利用者（３）が手で入力するのは手間を要するのでこれらの情報のいくつかもしくは全てを子局（２）に登録して利用する事も

できる。しかし、積極的に第三者に開示する情報ではないので、利用者（３）本人以外の人がアクセス出来ないようにして格納する。

【００１７】暗号鍵もしくは暗号鍵と暗号方式（１１）の生成と配布、管理

親局（１）が暗号鍵もしくは暗号鍵と暗号方式（１１）を何時生成もしくは選択して配布し、何時更新するのかはアプリケーションサービスによって異なってくる。基本的には親局（１）と子局（２）との間で鍵の生成、配布、更新に関する情報コマンドが交信されて親局（１）と子局（２）の間で、互いに一致した暗号鍵もしくは暗号鍵と暗号方式（１１）を記録、格納している。鍵を管理する情報コマンドとして下記のコマンドがある。

１．鍵の生成と配布要求
２．鍵の受信報告
３．鍵の更新要求
４．鍵の更新通達
５．鍵の更新報告

鍵の生成配布要求は、利用者（３）もしくは親局（１）のアプリケーションサービスから必要な時コマンドが発行される。鍵の更新通達は、管理の簡便さ、管理の必要上、図３で複数個の暗号鍵もしくは暗号鍵と暗号方式（１１）を一度に子局（２）に配布しておき、特定の利用回数もしくは特定の時間間隔もしくは特定の時間もしくは特定のアプリケーションサービスを実行した後等の、親局（１）と子局（２）間の共通の認識である鍵を管理する情報（１５）で、子局（２）が暗号鍵もしくは暗号鍵と暗号方式（１１）を変更した結果を報告する。この場合、親局（１）と子局（２）が常に共通の状況把握ができる状態の場合は子局（２）が鍵を変更するのと同じく、親局（１）が鍵の情報を更新できる。しかし、子局（２）の通達を受けるまで親局（１）が状況を把握できない場合、子局（２）は、更新が完了するまで、利用を保留しなければならない。例えば、子局（２）は現在使っている暗号鍵もしくは暗号鍵と暗号方式（１１）を設定した利用回数毎に使い捨て、次の暗号鍵もしくは暗号鍵と暗号方式（１１）に更新する場合、親局（１）と子局（２）の間で、利用回数に関する共通の概念が確認されていても、何回子局（２）で利用されたか子局（２）でないと状況の把握はできない場合、子局（２）で判断して暗号鍵もしくは暗号鍵と暗号方式（１１）を更新して、親局（１）へ鍵の更新通達を発行する。

【００１８】この発明で使用する暗号方式と暗号鍵は、既に世の中で研究された、共通鍵方式の暗号方式のいずれかを採用する。どのような暗号方式を選択するかは、アプリケーションサービスの特性もしくは事業性に合わせて選択する。

【００１９】この発明に於いて、暗号鍵もしくは暗号鍵と暗号方式（１１）の配布経路は、Ｎ人の参加者がある情報通信網の中で、（図４（ａ））で子局（２）が相互に鍵を配布する場合の配布経路はＮ＊（Ｎ－１）／２であるが、親局（１）と子局（２）の間だけの鍵配布経路は（図４（ｂ））でＮとなり、暗号鍵の配布経路は任意の相手に配布するのに比較して（Ｎ－１）／２倍だけ減少出来る。更に、（図４（ｃ））でＫ個の親局（１）を子局（２）と見なして新たな親局（１）を設け、今までの親局（１）を子局（２）として管理させる階層構造を持つ暗号情報交換網を設定すると、管理のスパンはＮとＫに減少し、暗号鍵もしくは暗号鍵と暗号方式（１１）の配布経路と配布の管理工数は大幅に簡素化される。

【００２０】子局（２）の登録と利用者（３）の登録

親局（１）が利用者（３）の登録を受け付ける時、利用者（３）が本人であることの確認は極めて重要である。ここでは、親局（１）、子局（２）、利用者（３）の間で、どの様な情報の交信が行われるのか、また、どの様な順序で情報が記録されるかを図（５）で示す。

１．最初に子局（２）からアプリケーションプログラムのダウンロード要求を親局（１）が受け付ける。親局（１）は、受付日時、ダウンロードするプログラムの管理番号、暗号鍵もしくは暗号鍵と暗号方式（１１）、子局（２）のＩＰ　Ａｄｄｒｅｓｓを確認情報として記録できる。インターネットのＩＰＡｄｄｒｅｓｓは一般に子局（２）に１対１に対応していないが、あるバンド幅の値を示したり、絶えず移動したり、固定した値だったり、ある特性を示すことを期待して記録する。

２．ダウンロードしたプログラム（５）を子局（２）にインストールし、子局（２）にプログラム固有の管理番号、暗号鍵もしくは暗号鍵と暗号方式（１１）が設定される。

３．利用者（３）は親局が指定する利用者属性情報（１０）を子局（２）を通して入力し、子局（２）の管理番号と共に親局（１）に送信する。

４．親局（１）は管理番号で暗号鍵もしくは暗号鍵と暗号方式（１１）を確認し、新たに登録の日時、利用者属性情報（１０）を記録し、子局識別記号（１２）及び、利用者識別記号（９）及び初期パスワード（１６）を生成し、記録する。

５．子局識別記号（１２）及び利用者識別記号（９）及び初期パスワード（１６）を暗号化して子局（２）へ送信する。

６．子局（２）は暗号化された子局識別記号（１２）及び、利用者識別記号（９）及び初期パスワード（１６）を復号化して、子局（２）に更新して格納する。

７．利用者（３）は、利用者識別記号（９）及び初期パスワード（１６）を確認する。

８．利用者（３）はパスワード（１６）の変更手続きを子局（２）を通して行い、親局（１）は変更を受け付け、記録を更新する。

９．利用者（３）は利用者識別記号（９）、パスワード（１６）を含む利用者属性情報（１０）を子局（２）を

通して入力し、子局（２）は子局の識別記（１２）と共に親局（１）に送信する。
１０．親局（１）は、利用者の識別記号（９）に対応したパスワード（１６）を含む利用者属性情報（１０）及び子局識別記号（１２）を記録する。
１１．通信網を介した情報だけで本人であることを確認するのは難しく、利用者の社会的な情報を示す、免許証、健康保険証、戸籍抄本等アプリケーションが指定する書類、又はそのコピーの送付を求め、既に送信された情報との確認を行い、書類を保管する。これで利用者（３）は子局（２）を経由して、親局（１）に登録される。
１２．親局（１）は利用者識別記号（９）並びに親局（１）の特徴を示す住所や電話番号、ＵＲＬ、ロゴマーク等を明示するカードを発行する。このカードは利用者（３）にトラブル時の連絡や、親局（１）を偽って働きかける場合の防止と親局（１）の宣伝を兼ねている。
【００２１】ダウンロードされたプログラムは一つの子局（２）だけで使用されるとは限らず、コピーされて、複数の子局（２）で利用される可能性が高いが、複数の子局（２）で利用されても、利用者（３）の登録時に暗号鍵もしくは暗号鍵と暗号方式（１１）が変更され問題にならない。一つの子局（２）で複数の利用者（３）が登録しても、複数の利用者識別記号（９）と、利用者識別記号（９）に対応した暗号鍵もしくは暗号鍵と暗号方式（１１）が親局（１）及び子局（２）に設定される。従って、一つの子局（２）を通じて、複数の利用者（３）がアプリケーションのサービスを利用できる。
【００２２】複数の子局（２）を経由して利用者（３）がサービスを利用する場合。利用者（３）が一つの子局（２）経由でサービスを利用するだけでなく、モーバイルの子局（２）や、別の場所にある子局（２）を通して、サービスを利用したい場合、登録した利用者（３）が本人か否か最初の登録と同じように本人を証明する社会的な情報の提出を受けて行う方法もあるが、利用者（３）にとって煩わしい。この不便を解消する通信網上での登録行為を図６に示す。
①　既に子局（２）Ａを通して、親局（１）に登録している利用者（３）ａが子局（２）Ｂを経由して、利用者識別記号（９）とパスワード（１６）を含むアプリケーションサービスが要求する利用者ａの属性情報（１０）を入力して複数個の登録申請手続きを親局（１）に行う。
②　親局（１）はこの手続きを受け付け、子局識別番号（１２）が子局（２）Ｂ経由で来たこと、及び利用者（３）ａが登録要求してきた事を既に登録済みの情報と突き合わせ確認し、記録する。
③　利用者（３）ａは既に登録されている子局（２）Ａ経由で認証手続きを行う。
④　親局（１）は利用者（３）ａが子局（２）Ａから受け取った認証依頼を確認して本人を認証する。
⑤　親局（１）は、子局（２）Ｂに利用者（３）ａの新しく生成した暗号鍵もしくは暗号鍵と暗号方式（１１）を配布し、親局暗号管理データ（１３）を更新する。
⑥　子局（２）Ｂは配布された暗号鍵もしくは暗号鍵と暗号方式（１１）で利用者（３）ａの利用者識別記号（９）対応した記録を作成する。この手続きが済んだ後、利用者（３）ａは子局（２）Ａもしくは子局（２）Ｂを経由してアプリケーションのサービスを利用できる。ここでは、子局（２）Ｂが既に子局として接続済みであるとして説明したが、子局（２）Ｂが未だ加入接続されていない場合は、子局（２）の加入接続手続きを行えば既に接続した場合と同じ扱いとなる。
【００２３】システムが破壊した場合の再登録方法
子局（２）のシステムが壊れる事がある。この場合の再登録は、利用者識別記号（９）と、パスワード（１６）、利用者属性情報（１０）を親局（１）が受信して、本人であると見なす方法もあるが、利用者識別記号（９）、パスワード（１６）を含む全ての利用者属性情報（１０）を盗まれた場合、別の子局（２）を通して親局（１）に加入接続し、本人に成りすます事が出来る。従って、社会的な情報を親局（１）に文書等で送付し、本人の確認をやり直す事になる。アプリケーションサービスを実行途中で、システムが一部破壊した場合、アプリケーションサービスの実行を破棄するか、文書等の別の手段で対策するか、もしくは、システムを復旧し、最初から登録をやり直して、アプリケーションサービスを実行する事になる。
【００２４】利用者の暗号鍵もしくは暗号鍵と暗号方式（１１）を親局（１）が管理しているとしても、子局（２）に記録された利用者の暗号鍵もしくは暗号鍵と暗号方式（１１）と親局（１）に記録された利用者の暗号鍵もしくは暗号鍵と暗号方式（１１）の持ち方の関係を明確にしておく必要がある。
【００２５】襷掛け配布
図７に親局（１）で記録している利用者の暗号鍵もしくは暗号鍵と暗号方式（１１）と子局（２）で記録している暗号鍵もしくは暗号鍵と暗号方式（１１）との間の依存関係を示す。既に子局（２）に格納された利用者（３）の暗号鍵もしくは暗号鍵と暗号方式（１１）を暗号鍵$_{k-1}$、暗号方式$_{k-1}$とすると、新たに親局（１）が子局（２）に配布する暗号鍵もしくは暗号鍵と暗号方式（１１）は、既に子局（２）に格納された暗号鍵$_{k-1}$、暗号方式$_{k-1}$で暗号化して子局（２）に送信し、子局（２）はそれを復号化して暗号鍵$_{k}$、暗号方式$_{k}$へ更新する。これ以降、新しい鍵の配布を受けるまでの間、子局（２）を通じて送受信される情報は暗号鍵$_{k}$、暗号方式$_{k}$で暗号化、複号化される。暗号鍵もしくは暗号鍵と暗号方式（１１）と同時に暗号情報を受信した場合、その暗号は既に登録されている暗号鍵$_{k-1}$、

暗号方式$_{k-1}$　で復号化する。このように、既に送信済みの暗号鍵もしくは暗号鍵と暗号方式（１１）を使って暗号化と復号化を行うので、襷掛けの暗号鍵もしくは暗号鍵と暗号方式（１１）の利用形態となる。親局（１）と子局（２）の間で、暗号鍵もしくは暗号鍵と暗号方式（１１）の襷掛けに利用できる関係は、鍵の配布と暗号情報の交信に時間的なずれが生じセキュリティ確保上、有利に働く。

【００２６】暗号鍵のパラレル配信方式

図８に親局（１）が暗号化した暗号鍵もしくは暗号鍵と暗号方式（１１）を子局（２）に配布し、配布された暗号を子局（２）の中で復号化して、暗号鍵もしくは暗号鍵と暗号方式（１１）を子局（２）の中に格納する。前に配布済みの暗号鍵もしくは暗号鍵と暗号方式（１１）を使用せず配布した暗号鍵もしくは暗号鍵と暗号方式（１１）で情報を暗号化、復号化する。

【００２７】親局（１）と子局（２）及び利用者（３）から成る暗号情報交換方式を利用する情報交換の方式は、次の３つの形式を設定する。

１　親局（１）が利用者（３）の情報を中継して情報の交換を行う。

２　利用者（３）間で直接情報の交換を行う。

３　親局（１）と利用者（３）間で情報の交換を行う。

利用者（３）である事を確認した後、更新する情報は、平文を暗号化して情報の交信を行う場合と、平文の儘交信を行う場合とがある。情報交信として、トラブル時の情報交換など、管理上発生する情報の交換はアプリケーションサービスの実行を支えるために、目的とする情報交換以外にも発生するが、ここでは利用者（３）がアプリケーションサービスを利用する上で行う情報交換についてのみ説明する。

【００２８】中継情報交換：図９に親局（１）が子局（２）Ａと子局（２）Ｂとの間で情報を取り次いで子局（２）Ａ、Ｂ間で情報の中継交信を行う場合を示す。利用者（３）ａの暗号鍵もしくは暗号鍵と暗号方式（１１）で暗号化した送達情報と送信先の利用者（３）の宛先を親局（１）宛に送信する。受信した親局（１）は暗号を復号化して、子局（２）Ｂの利用者（３）ｂの暗号鍵もしくは暗号鍵と暗号方式（１１）で送達情報を暗号化して、利用者（３）ｂが登録されている子局（２）Ｂ宛に送信する。子局（２）Ｂで受信した利用者（３）ｂは情報を復号化して、受信情報の内容を理解する。子局（２）Ａと子局（２）Ｂ間で直接情報の送受信を行わず、親局（１）を中継して間接的に情報の交信を行う。

【００２９】中継情報交換の場合、親局（１）で情報の暗号化、復号化の中継作業を行うため、手間を要するが、そのために得られる利点もある。

１　間接的な情報取引の為に、利用者（３）ａの利用者属性情報（１０）は親局（１）で確認するにとどめ、用件に関する情報だけを利用者（３）ｂに伝える事で、匿名の情報伝達が可能となる。

２　親局（１）が子局（２）Ａ、Ｂ間の中継情報交換を行う場合、図１０の利用者（３）ａの情報を親局（１）が受信するタイミングと、利用者（３）ｂの情報を受信するタイミングが一致しない場合、アプリケーションサービスの処理を一時保留し、双方の情報が揃ってからアプリケーションサービスの処理を実行する。

【００３０】利用者（３）間で直接情報の交信を行う場合：親局（１）を介さないで直接子局（２）間で暗号情報を交信したい場合、図１１で子局（２）Ａを通じて利用者（３）ａは利用者（３）ｂとの直接交信要求と、暗号鍵もしくは暗号鍵と暗号方式（１１）もしくはそれに代わる確認用の暗号確認情報（２３）の配布依頼をする。親局（１）は、利用者（３）ａ、及び利用者（３）ｂ共通の暗号鍵もしくは暗号鍵と暗号方式（１１）もしくはそれに代わる暗号確認情報（２３）を生成もしくは選択し子局（２）Ａ及び、子局（２）Ｂへ配布する。双方の子局（２）で複号化した暗号鍵もしくは暗号鍵と暗号方式（１１）もしくはそれに代わる暗号確認情報（２３）を格納し利用者（３）ａ、ｂ間で暗号情報を送受信し、復号化して内容を確認し、情報の交信を行う。

【００３１】利用者（３）で情報の送信元と受信元の間で暗号情報の送受信が行われる場合、送信元利用者（３）から単数もしくは複数の送信先利用者（３）へ暗号鍵もしくは暗号鍵と暗号方式（１１）の配布要求が親局（１）へなされ、親局（１）は、送信先の利用者（３）の暗号鍵もしくは暗号鍵と暗号方式（１１）を送信元の利用者（３）の利用者識別記号（９）が格納されている子局（２）へ送信し、送信元の利用者の識別記号（９）は情報を暗号化して、送信先へ送信し、送信先の利用者（３）が暗号を複合化して情報交信がなされる。

【００３２】親局（１）と利用者（３）間で情報の交信を行う：利用者（３）が子局（２）を通じて直接親局（１）との間で情報の交信を行う場合もある。図１２で利用者（３）のＡ１は子局（２）Ａを通して、親局（１）と直接情報の交信を行う。

【００３３】

【実施例】

デリバリー取引

図１３に通信網を介して商品の配送を行う商品売買取引システムの例を示す。親局（１）は購買者からの注文を販売者に取次ぎ、売買が合意されると取引の決済を行う。子局（２）の購買者は購入する商品の注文を行い、子局（２）の販売者は注文を承けて、商品を直接発送先へ発送する。親局（１）の取引取次・決済機関に加入接続した複数の子局に登録した購買者と複数の子局に登録した販売者は商取引通信網を構成する。親局（１）が利用者（３）の情報を中継して情報の交換を行う場合の実施例に当たる。図１３で取引の手続きを追うと、

①購買者の取引開始依頼を利用者識別記号（９）及び利

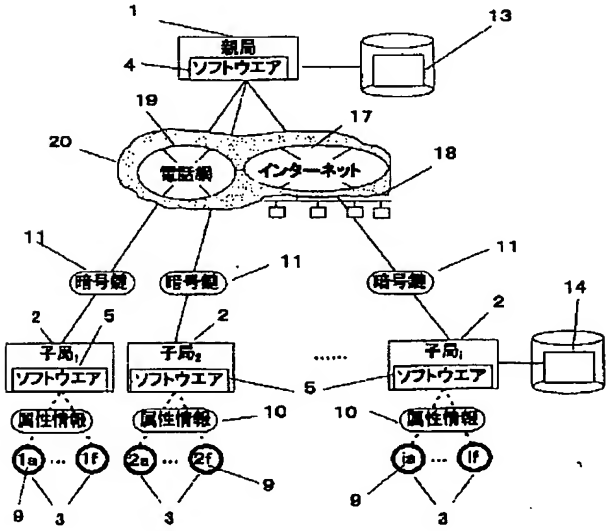
用者属性情報（１０）及び子局識別記号（１２）と一緒に中継取次・決済機関に送信し、中継取次・決済機関はこれを復号化する。利用者識別記号（９）及び利用者属性情報（１０）及び子局識別記号（１２）で購買者を確認する。
②中継取次・決済機関は取引番号と購買者の暗号鍵もしくは暗号鍵と暗号方式（１１）を生成し購買者に配布する。受信した購買者は子局（２）で暗号鍵もしくは暗号鍵と暗号方式（１１）が更新される。
③購買者は販売者の子局（２）のＵＲＬ（Ｕｎｉｖｅｒｓａｌ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）と購入したい商品情報、及び購買者の属性情報を暗号化して中継取次・決済機関に送信する。中継取次・決済機関は暗号を復号化して、購買者の認証を行い、与信を確認する。
④販売者の暗号鍵もしくは暗号鍵と暗号方式（１１）で購買者の購買仕様を暗号化して、販売者の子局（２）に送信する。このとき、商品の取引に関わる情報だけを販売者に中継して送信するので、購買者は匿名で商品の購入が出来る。販売者の暗号鍵もしくは暗号鍵と暗号方式（１１）は親局（１）の中継取次・決済機関が任意の考え方で生成・配布して変更する。例えば設定した取引き回数、もしくは設定した時間間隔等の更新が考えられる。
⑤販売者は注文の仕様を確認し、中継取次・決済機関に受注連絡を商品の発送予定日と一緒に送信する。中継取次・決済機関は暗号を復号化し、注文と一致しているか否か確認し、内部決済処理を行う。
⑥中継取次・決済機関は売買成立と発送予定日を購買者に送信する。
⑦販売者から商品の発送連絡が中継取次・決済機関に送信されると、中継取次・決済機関は購買者及び販売者の間で取引の決済を行う。
商品の引き渡しを伴う取引を通信網で行う場合の決済は中継取次・決済機関を中継する事で、販売者から商品発送の情報を受けた後、決済を行うので相対取引と同じタイミングで決済が可能となり店頭で商品を現品で受け取って代金を支払うのと同じ様な相対取引決済ができ、購買者と販売者の間の取引に伴う商品を送ったが、お金が回収できないとか、お金を送ったが商品が発送されないとか言うリスクを軽減できる。
【００３４】情報サービス
図１４にデター提供等のサービス取引を通信網を用いて行う場合を示す。
①サービス利用者はサービス提供者の子局（２）のＵＲＬ（ＵｎｉｖｅｒｓａｌＲｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）とサービス利用者属性情報（１０）を暗号化して、サービス利用請求をサービス仲介機関に送信する。サービス仲介機関は暗号を復号化し、サービス利用者の認証と、信用の確認を行う。
②サービス仲介機関は暗号鍵もしくは暗号鍵と暗号方式（１１）を生成もしくは選択し、更にサービス利用者サービス提供者共通の取引番号を生成し、サービス利用者にサービス提供者の暗号鍵もしくは暗号鍵と暗号方式（１１）で暗号化した取引番号とサービス利用者の暗号鍵もしくは暗号鍵と暗号方式（１１）を暗号化して送信し、サービス提供者に取引番号を暗号化して送信する。暗号化された取引番号は暗号確認情報（２３）を示す。サービス利用者は送信された取引番号及び暗号鍵もしくは暗号鍵と暗号方式（１１）を格納する。
③サービス利用者はサービス提供者に取引番号を送信し、サービス提供者が暗号化された取引番号を複号化して確認する。
④サービス利用者はサービス提供者からデータサービスを直接受ける。
⑤サービス料金は、サービス提供者からサービス仲介機関に料金請求がなされて、サービス仲介機関もしくは決済機関が決済を行う。
決済引き落としを承諾したサービス利用者と、サービス提供者が、直接、サービス利用に関する決済の問題を処理しなくても、サービス仲介機関を介する事で、小口の費用の決済が可能で簡便にサービスが受けられる。
【００３５】図１５に暗号情報交換方式を利用したホームバンキングを示す。金融機関Ｃに預金口座を開設した口座開設者は、子局（２）を通じて金融機関Ｃから配布された暗号鍵もしくは暗号鍵と暗号方式（１１）で、利用者識別記号（９）及び利用者属性情報（１０）及び子局識別記号（１２）と、振り込み情報と一緒に暗号化して親局（１）の金融機関に送信し、親局（１）の金融機関で復号化して、口座開設者を認証し、同じ金融機関Ｃの他の口座開設者もしくは他の金融機関Ｄの口座開設者に送金処理が行われる。
【００３６】親書の配送
図１６に電子情報管理機構による親書の確実な配達を行うシステムを示す。電子情報管理機構にメール送受信者は登録した子局（２）通じてメールアドレス毎にパスワード（１６）を随時設定する。設定されたパスワード（１６）は、電子情報管理機構に送信される。
①発信者ａが子局（２）を通じて電子情報管理機構に送信先のメールアドレスを暗号化して送信し、親書の送信要求を行う。
②電子情報管理機構は子局（２）Ａの発信者ａに受信者ｂの暗号鍵もしくは暗号鍵と暗号方式（１１）を暗号化して送信する。
③発信者ａは親書を暗号化して、受信者ｂに送信する。
④受信者ｂの復号化が成功すると、子局（２）Ｂは受信復号化確認情報を電子情報管理機関に送信し、設定された暗号鍵もしくは暗号鍵と暗号方式（１１）で受信できる回数のカウンターを一つ減ずる。カウンターの値が設定された値に達すると、その暗号鍵もしくは暗号鍵と暗号方式（１１）は図１６でｅｆｇからｈｉｊへ更新され

ｅｆｇは消去される。
⑤電子情報管理機構から子局（２）の発信者に送達連絡を行う。電子情報管理機構は、あらかじめ、メールアドレス毎に複数の暗号鍵もしくは暗号鍵と暗号方式（１１）を配布し、設定された回数だけ受信者が子局（２）で親書を受信すると、その暗号鍵もしくは暗号鍵と暗号方式（１０）は子局（２）から消去される。発信者ａと受信者ｂとの間で暗号化された親書が届けられた事を電子情報管理機構を経由して連絡し、親書の送達が確認できる。
【００３７】イントラネット
図１７に企業内でのイントラネットの情報管理の例を示す。ＬＡＮ（１８）に接続された子局（２）$_{11}$・・子局（２）$_{1k}$とインターネットを介して接続された子局（２）２１・・子局（２）２ｊ及び、リモートアクセスで接続された子局（２）ｊｐから成るＷＡＮ（２０）を経由して接続されたイントラネットで、サーバにアクセスする情報をファイアウオール（２２）で防御するだけでなく、親局（１）のサーバが接続された子局（２）に生成し配布する暗号鍵もしくは暗号鍵と暗号方式（１１）を利用することによって、親局（１）のサーバーを経由する全ての情報のセキュリティが保てるシステムが構築出来る。ファイアウオール（２２）で外部からの情報に対するセキュリティを強化しても、組織が大きくなると、ファイアウオールの内部でのセキュリティを如何に確保するかが大きな課題であるが、使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）の管理方式はこの問題を解決してくれる。
【００３８】図１８で共通の暗号鍵もしくは暗号鍵と暗号方式（１１）を使用する場合を示す。親局（１）から配布された共通の暗号鍵もしくは暗号鍵と暗号方式（１１）を子局ａ、子局ｂ、子局ｃが共有し、情報を関係者だけで交信できる。暗号鍵もしくは暗号鍵と暗号方式（１１）の更新はアプリケーションサービスによって設定されるし、メンバーの変更に柔軟に対応できる。掲示板を共通の暗号鍵もしくは暗号鍵と暗号方式（１１）を使う場合も、関係者の認証がパスワード（１６）のみに比較してセキュリティ機能が高く、問題を制限して討論する場合などに利用できる。
【００３９】
【発明の効果】任意の交信相手全ての人に暗号鍵を安全に渡すために、公開鍵、秘密鍵方式が実行されているが、親局と子局の関係で電子情報網を構築して親局と子局及び登録された利用者の間だけで暗号情報の交換を行う事で目的が達成される場合、親局が全ての情報を管理できるために、使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）で管理すれば、利用者は暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）の存在さえ意識せず、セキュリティの個人での管理が簡便になる。
【００４０】一方、ＷＡＮを経由した外部からの犯罪行為に対して、ファイアウオールで外部からのアクセスを制限し、セキュリティを確保している。しかし、組織が大きくなると外部からの不正な情報アクセスに対する防御だけでなく、内部での情報網のセキュリティの重要性が高まってくるが、ファイアウオールでは防御できない。Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓ　Ｗｏｒｄは内部の情報通信網でも本人の認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）に関して効果があるが、情報の機密性に対応出来ない。使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）を使った暗号情報交換方式はイントラネット等で、内外のアクセスを問わずセキュリティが確保できる。
【００４１】インターネットは本来クライアントサーバシステムで構成されているので、親局と子局の関係で情報通信網の利用システムを構成できる場合が多く、使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）と暗号方式を使った、暗号情報の交換方式は幅広い分野での使い方が期待できる。
【００４２】親局（１）と子局（２）及び利用者（３）の関係の間で管理する使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）の暗号情報交換方式を使用して、専用回線を使ったプライベート網とほぼ同等以上のセキュリティを保ちながら、利用者は暗号鍵もしくは暗号鍵と暗号方式の内容を知らなくても、オープンで安価なインターネットや、公衆電話網を利用して、安全なプライベート網を構築出来る。

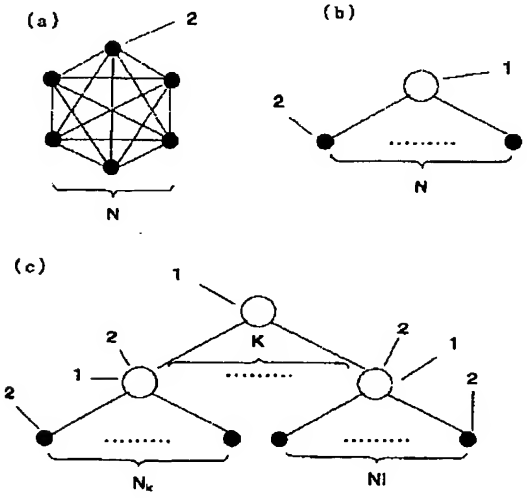
【図面の簡単な説明】
【図１】利用者と子局と親局から成る情報通信網で、使い捨て暗号鍵（ＴｈｒｏｗＡｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）で情報を管理するシステム構成
【図２】利用者、子局、親局の間で、暗号情報交換を行う機能の分担
【図３】鍵を管理する情報で、複数個用意した暗号鍵もしくは暗号鍵と暗号方式の更新を行う方式
【図４】（ａ）Ｎ人の間で暗号鍵を渡す経路の数
（ｂ）親局と子局の関係を構成し、Ｎ人の間で暗号鍵を渡す経路の数
（ｃ）親局と子局の関係を構成し、更に親局を子局としてその上に親局を構成し、階層的な親局と子局を構成したときの暗号鍵の経路の数
【図５】利用者が子局を通して親局へ登録する方式
【図６】利用者が通信網の情報交信だけで複数の子局を通して親局へ登録する
【図７】親局と子局の間でたすき掛けで生成する使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）の管理方式
【図８】親局から子局へ送信した暗号鍵もしくは暗号鍵と暗号方式で、暗号化に使用する使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）

の管理方式
【図９】親局を中継して、子局の間で暗号化した情報の送受信を行う暗号情報交換方式
【図１０】親局が子局間の情報が揃うのを待って、子局間に関わる情報処理を行うアプリケーションサービスシステム。
【図１１】親局が子局間共通の暗号鍵もしくは暗号鍵と暗号方式を生成もしくは選択して配布する暗号情報交換方式
【図１２】使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）で親局と子局が直接暗号情報の交信を行うシステム
【図１３】使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）を使って商品の配送を伴う通信網上での商取引システム
【図１４】使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）を使って情報サービスを行うシステム
【図１５】口座開設者が金融機関との間でオープンなネットワークを介してホームバンキングを行うシステム。
【図１６】使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）を使って親書の配送を行うシステム
【図１７】使い捨て暗号鍵（Ｔｈｒｏｗ　Ａｗａｙ　Ｅｎｃｒｙｐｔｉｃａｌ　ｋｅｙ）を使ってＬＡＮ、ＷＡＮを介したイントラネットでファイアウオールの内外を問わず、セキュリティの高い情報交信を可能とするシステム
【図１８】共通の暗号鍵もしくは暗号鍵と暗号方式を使った情報交換方式
【符号の説明】
１．　親局
２．　子局
３．　利用者
４．　暗号情報交換機能を使う親局用のアプリケーションソフトウエ
５．　暗号情報交換機能を使う子局用のアプリケーションソフトウエ
６．　暗号情報交換機能の親局の分担機能
７．　暗号情報交換機能の子局の分担機能
８．　暗号情報交換機能の利用者の分担機能
９．　利用者識別記号
１０．利用者属性情報
１１．暗号鍵もしくは暗号鍵と暗号方式
１２．子局識別記号
１３．親局暗号鍵管理データ
１４．子局暗号鍵管理データ
１５．鍵を更新管理する情報
１６．パスワード
１７．インターネット
１８．ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　ｎｅｔｗｏｒｋ）
１９．公衆電話網
２０．ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　ｎｅｔｗｏｒｋ）
２１．情報パケット
２２．ファイアウオール
２３．暗号確認情報

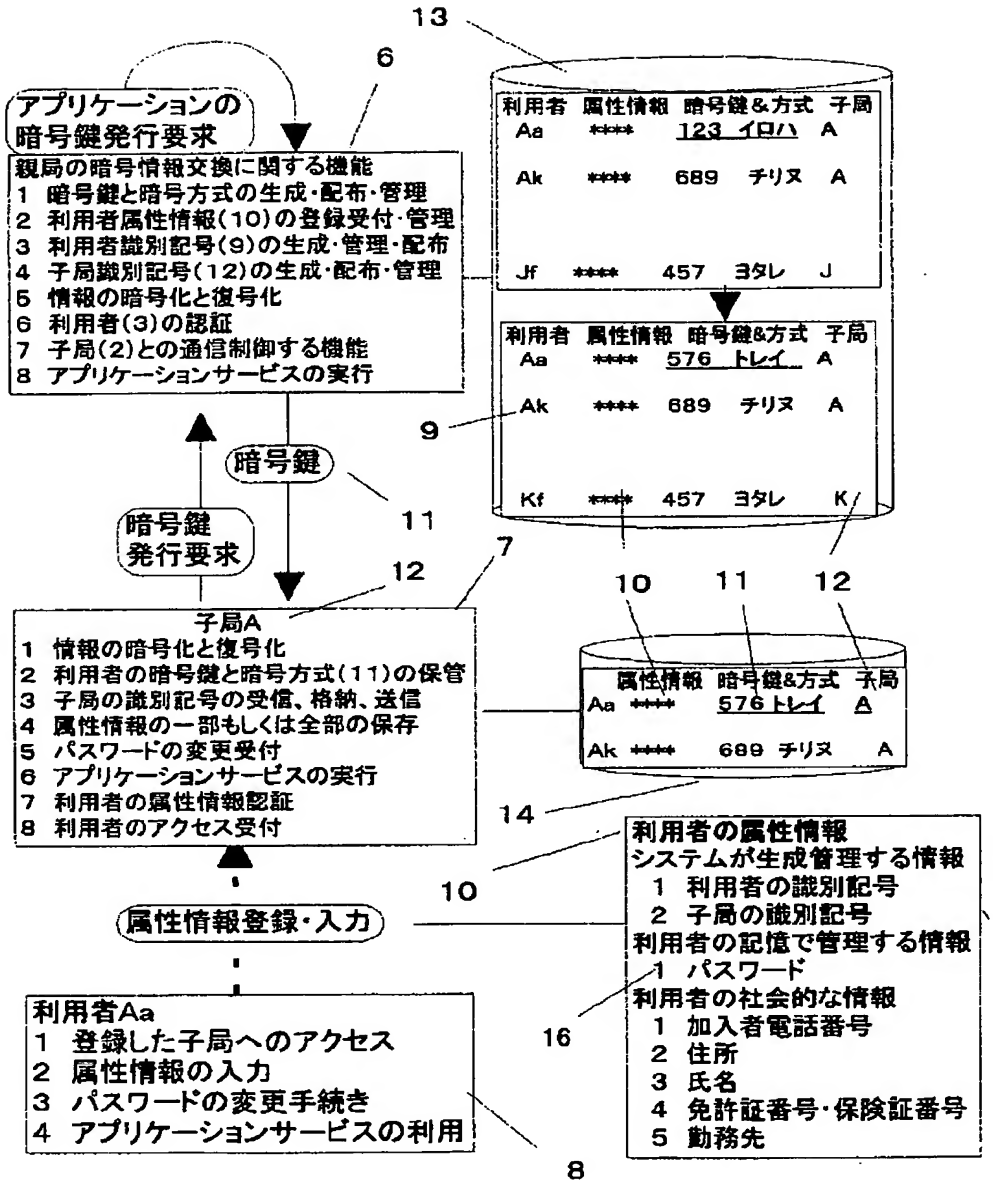
【図１】



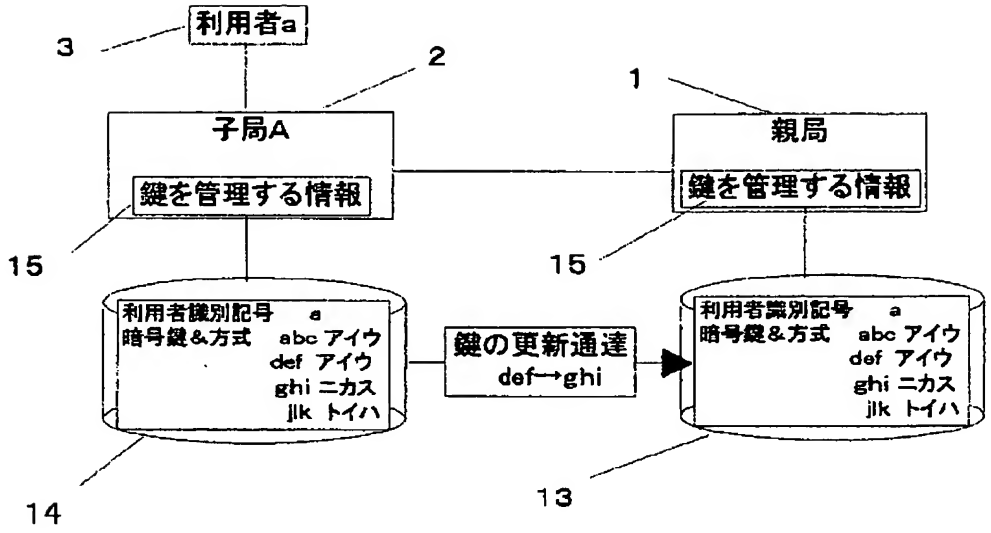
【図４】



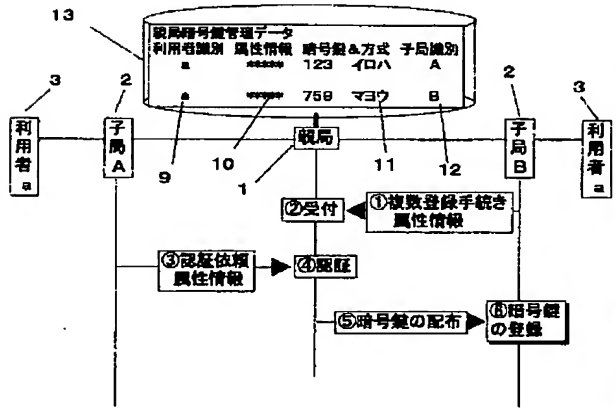
【図２】


13
6
アプリケーションの
暗号鍵発行要求
親局の暗号情報交換に関する機能
1 暗号鍵と暗号方式の生成・配布・管理
2 利用者属性情報(10)の登録受付・管理
3 利用者識別記号(9)の生成・管理・配布
4 子局識別記号(12)の生成・配布・管理
5 情報の暗号化と復号化
6 利用者(3)の認証
7 子局(2)との通信制御する機能
8 アプリケーションサービスの実行
利用者 属性情報 暗号鍵&方式 子局
Aa **** 123 イロハ A
Ak **** 689 チリヌ A
Jf **** 457 ヨタレ J
利用者 属性情報 暗号鍵&方式 子局
Aa **** 576 トレイ A
Ak **** 689 チリヌ A
Kf **** 457 ヨタレ K
9
暗号鍵
11
暗号鍵
発行要求
7
12
子局A
1 情報の暗号化と復号化
2 利用者の暗号鍵と暗号方式(11)の保管
3 子局の識別記号の受信、格納、送信
4 属性情報の一部もしくは全部の保存
5 パスワードの変更受付
6 アプリケーションサービスの実行
7 利用者の属性情報認証
8 利用者のアクセス受付
10
11
12
属性情報 暗号鍵&方式 子局
Aa **** 576 トレイ A
Ak **** 689 チリヌ A
14
利用者の属性情報
システムが生成管理する情報
1 利用者の識別記号
2 子局の識別記号
利用者の記憶で管理する情報
1 パスワード
利用者の社会的な情報
1 加入者電話番号
2 住所
3 氏名
4 免許証番号・保険証番号
5 勤務先
10
16
属性情報登録・入力
利用者Aa
1 登録した子局へのアクセス
2 属性情報の入力
3 パスワードの変更手続き
4 アプリケーションサービスの利用
8

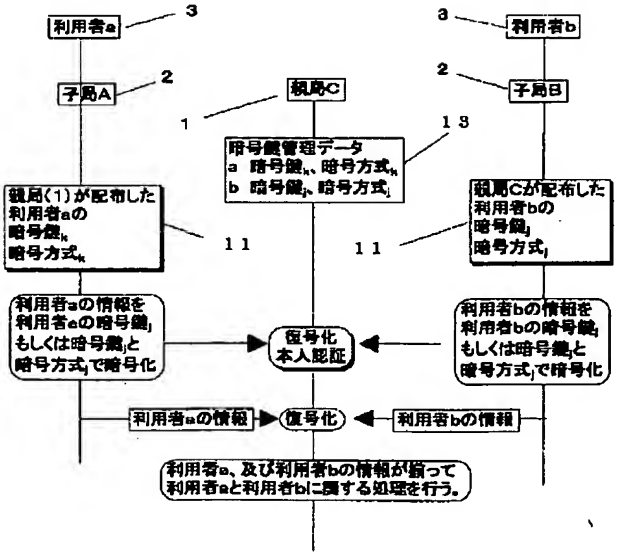
【図３】


利用者a
3
2
1
子局A
鍵を管理する情報
親局
鍵を管理する情報
15
15
利用者識別記号　a
暗号鍵&方式　abc アイウ
def アイウ
ghi ニカス
jlk トイハ
鍵の更新通達
def→ghi
利用者識別記号　a
暗号鍵&方式　abc アイウ
def アイウ
ghi ニカス
jlk トイハ
14
13

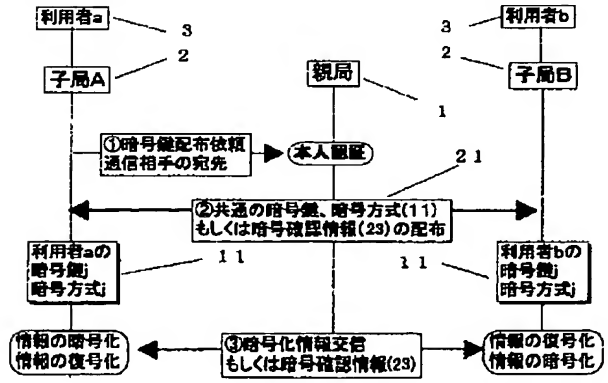
【図６】


13
親局暗号鍵管理データ
利用者識別　属性情報　暗号鍵&方式　子局識別
a　******　123　イロハ　A
a　******　759　マヨウ　B
利用者a
3
子局A
2
親局
1
子局B
2
利用者a
3
9
10
11
12
②受付
①複数登録手続き
属性情報
③認証依頼
属性情報
④認証
⑤暗号鍵の配布
⑥暗号鍵の登録

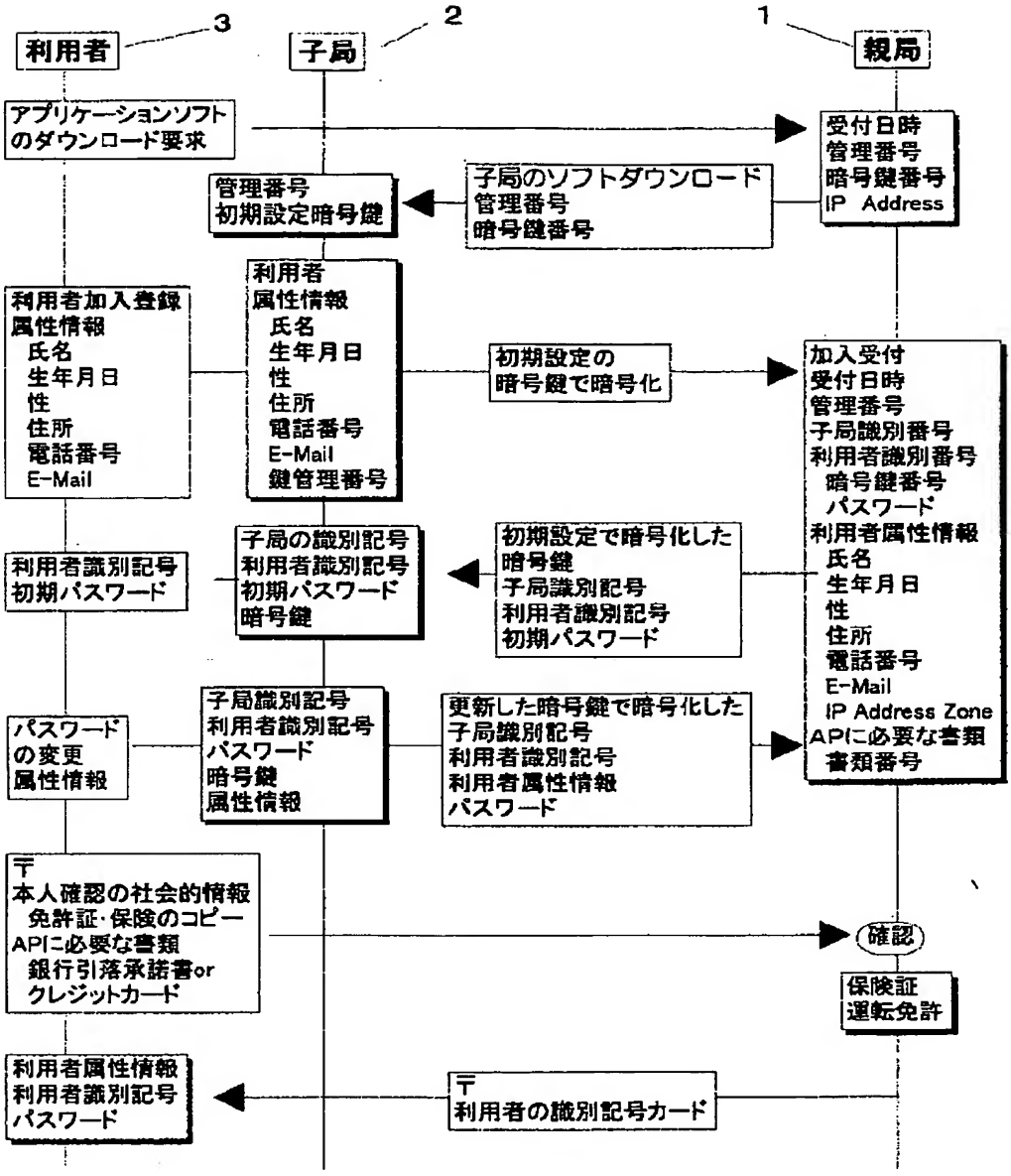
【図１０】


利用者a
3
子局A
2
親局C
1
暗号鍵管理データ
a　暗号鍵k、暗号方式k
b　暗号鍵j、暗号方式j
13
利用者b
3
子局B
2
親局(1)が配布した
利用者aの
暗号鍵k
暗号方式k
11
親局Cが配布した
利用者bの
暗号鍵j
暗号方式j
11
利用者aの情報を
利用者aの暗号鍵j
もしくは暗号鍵kと
暗号方式jで暗号化
復号化
本人認証
利用者bの情報を
利用者bの暗号鍵j
もしくは暗号鍵kと
暗号方式jで暗号化
利用者aの情報
復号化
利用者bの情報
利用者a、及び利用者bの情報が揃って
利用者aと利用者bに関する処理を行う。

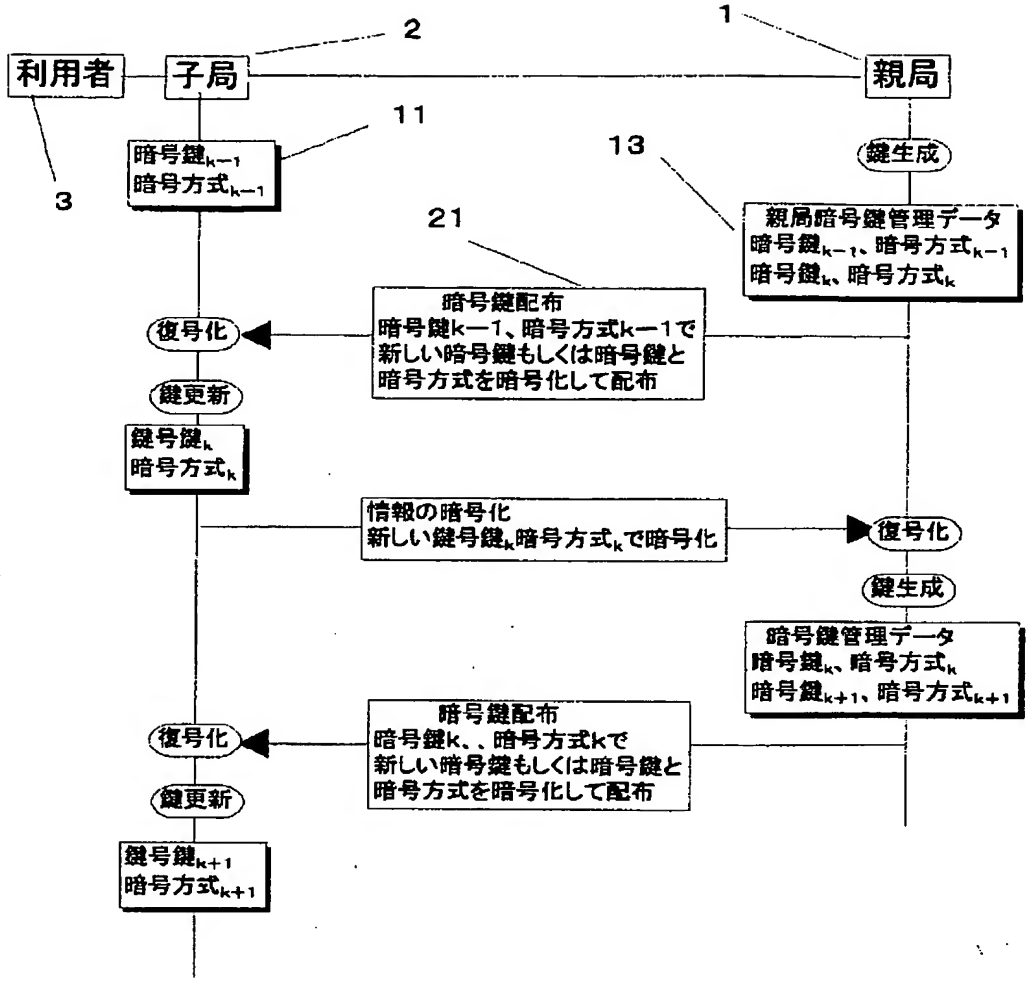
【図１１】


利用者a
3
子局A
2
親局
1
3
利用者b
2
子局B
①暗号鍵配布依頼
通信相手の宛先
本人認証
21
②共通の暗号鍵、暗号方式(11)
もしくは暗号確認情報(23)の配布
利用者aの
暗号鍵j
暗号方式j
11
11
利用者bの
暗号鍵j
暗号方式j
情報の暗号化
情報の復号化
③暗号化情報交信
もしくは暗号確認情報(23)
情報の復号化
情報の暗号化

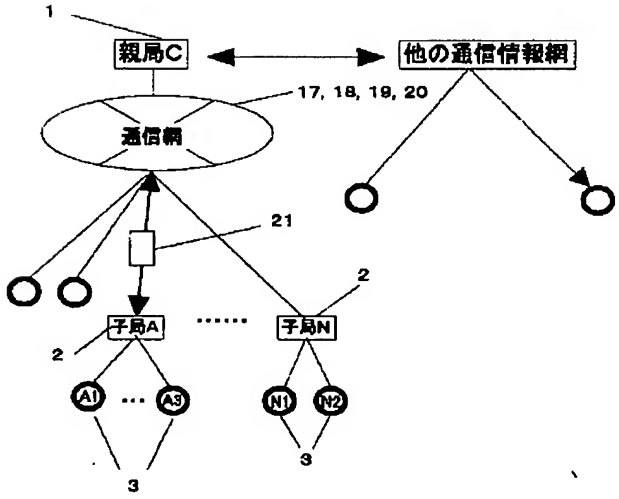
【図５】


利用者
3
子局
2
親局
1
アプリケーションソフトのダウンロード要求
受付日時
管理番号
暗号鍵番号
IP Address
管理番号
初期設定暗号鍵
子局のソフトダウンロード
管理番号
暗号鍵番号
利用者加入登録
属性情報
氏名
生年月日
性
住所
電話番号
E-Mail
利用者
属性情報
氏名
生年月日
性
住所
電話番号
E-Mail
鍵管理番号
初期設定の
暗号鍵で暗号化
加入受付
受付日時
管理番号
子局識別番号
利用者識別番号
暗号鍵番号
パスワード
利用者属性情報
氏名
生年月日
性
住所
電話番号
E-Mail
IP Address Zone
APに必要な書類
書類番号
利用者識別記号
初期パスワード
子局の識別記号
利用者識別記号
初期パスワード
暗号鍵
初期設定で暗号化した
暗号鍵
子局識別記号
利用者識別記号
初期パスワード
パスワード
の変更
属性情報
子局識別記号
利用者識別記号
パスワード
暗号鍵
属性情報
更新した暗号鍵で暗号化した
子局識別記号
利用者識別記号
利用者属性情報
パスワード
〒
本人確認の社会的情報
免許証･保険のコピー
APに必要な書類
銀行引落承諾書or
クレジットカード
確認
保険証
運転免許
利用者属性情報
利用者識別記号
パスワード
〒
利用者の識別記号カード

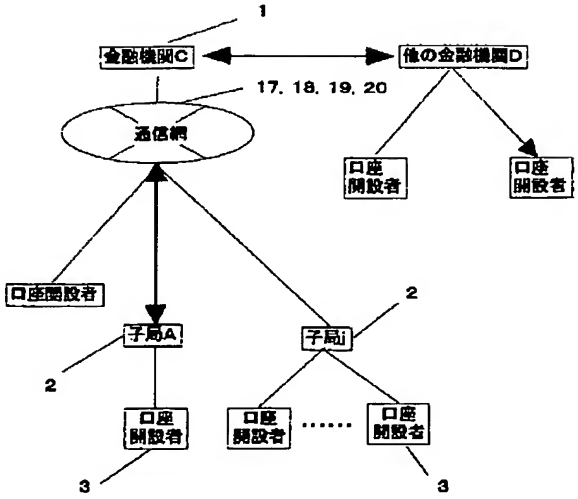
【図７】


利用者
子局
親局
2
1
3
11
13
21
暗号鍵k−1
暗号方式k−1
鍵生成
親局暗号鍵管理データ
暗号鍵k−1、暗号方式k−1
暗号鍵k、暗号方式k
暗号鍵配布
暗号鍵k−1、暗号方式k−1で
新しい暗号鍵もしくは暗号鍵と
暗号方式を暗号化して配布
復号化
鍵更新
鍵号鍵k
暗号方式k
情報の暗号化
新しい鍵号鍵k暗号方式kで暗号化
復号化
鍵生成
暗号鍵管理データ
暗号鍵k、暗号方式k
暗号鍵k+1、暗号方式k+1
暗号鍵配布
暗号鍵k、、暗号方式kで
新しい暗号鍵もしくは暗号鍵と
暗号方式を暗号化して配布
復号化
鍵更新
鍵号鍵k+1
暗号方式k+1

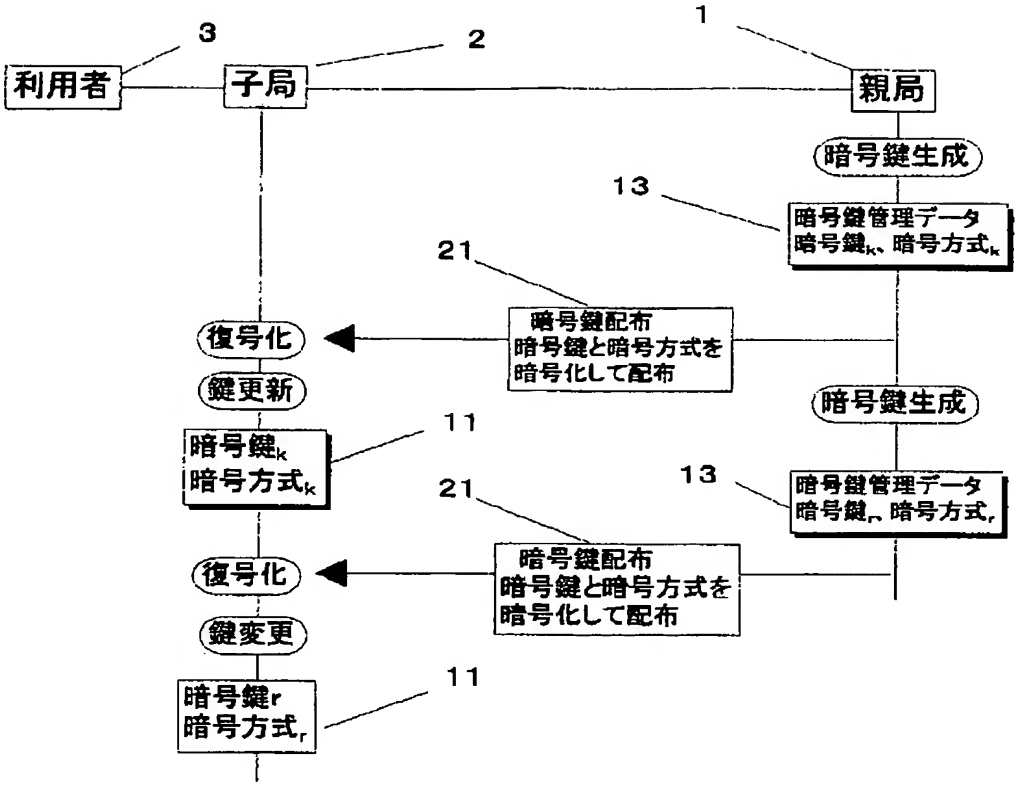
【図１２】


1
親局C
他の通信情報網
17, 18, 19, 20
通信網
21
2
子局A
子局N
2
A1
A3
N1
N2
3
3

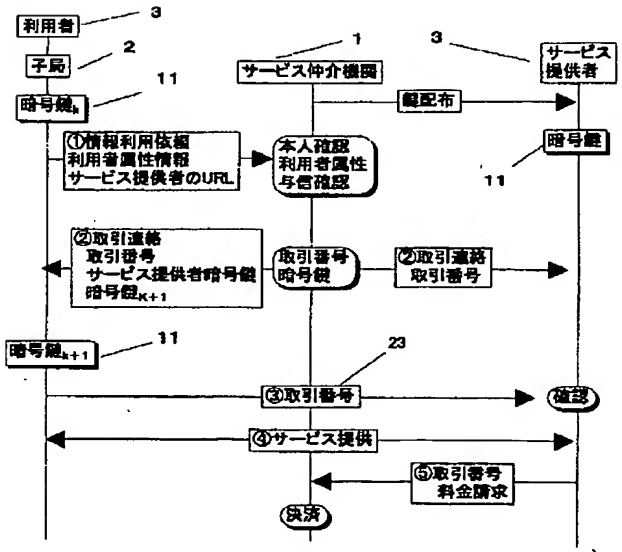
【図１５】


1
金融機関C
他の金融機関D
17, 18, 19, 20
通信網
口座開設者
口座開設者
口座開設者
2
子局A
子局j
2
口座開設者
口座開設者
口座開設者
3
3

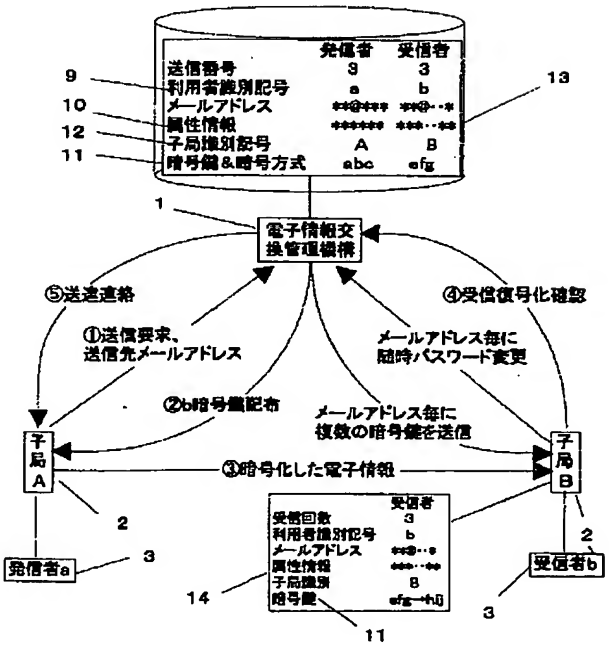
【図８】


3
2
1
利用者
子局
親局
暗号鍵生成
13
暗号鍵管理データ
暗号鍵k、暗号方式k
21
暗号鍵配布
暗号鍵と暗号方式を
暗号化して配布
復号化
鍵更新
暗号鍵k
暗号方式k
11
暗号鍵生成
13
暗号鍵管理データ
暗号鍵r、暗号方式r
21
暗号鍵配布
暗号鍵と暗号方式を
暗号化して配布
復号化
鍵変更
暗号鍵r
暗号方式r
11

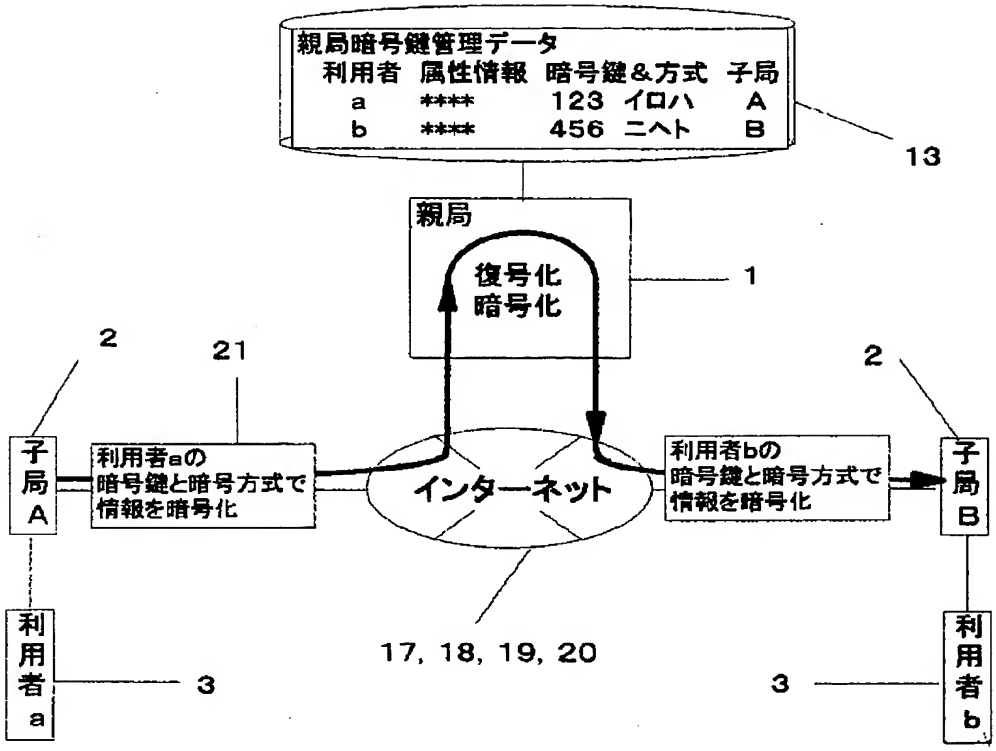
【図１４】


利用者
3
子局
2
11
暗号鍵k
①情報利用依頼
利用者属性情報
サービス提供者のURL
サービス仲介機関
1
本人確認
利用者属性
与信確認
3
サービス
提供者
鍵配布
暗号鍵
11
②取引連絡
取引番号
サービス提供者暗号鍵
暗号鍵k+1
取引番号
暗号鍵
②取引連絡
取引番号
暗号鍵k+1
11
23
③取引番号
確認
④サービス提供
⑤取引番号
料金請求
決済

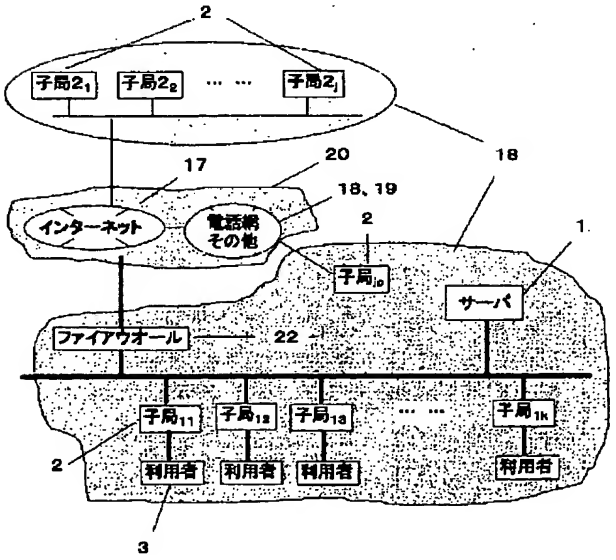
【図１６】


発信者
受信者
送信番号
3
3
利用者識別記号
a
b
メールアドレス
属性情報
子局識別記号
A
B
暗号鍵&暗号方式
abc
efg
9
10
12
11
13
1
電子情報交
換管理機構
⑤送達連絡
④受信復号化確認
①送信要求、
送信先メールアドレス
メールアドレス毎に
随時パスワード変更
②b暗号鍵配布
メールアドレス毎に
複数の暗号鍵を送信
子
局
A
③暗号化した電子情報
子
局
B
2
2
発信者a
3
受信者b
3
受信回数
3
利用者識別記号
b
メールアドレス
属性情報
子局識別
B
暗号鍵
14
11

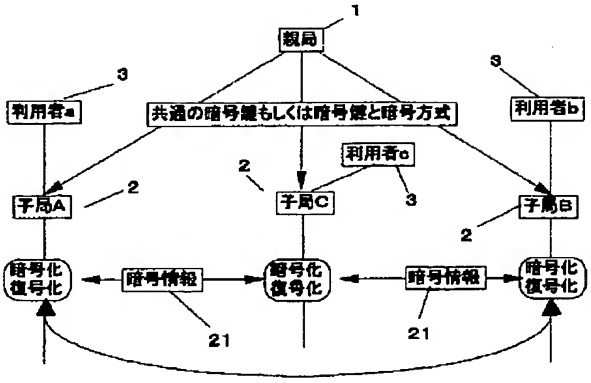
【図９】


親局暗号鍵管理データ
利用者 属性情報 暗号鍵&方式 子局
a **** 123 イロハ A
b **** 456 ニヘト B
13
親局
復号化
暗号化
1
2
21
2
子局A
利用者aの
暗号鍵と暗号方式で
情報を暗号化
インターネット
利用者bの
暗号鍵と暗号方式で
情報を暗号化
子局B
17, 18, 19, 20
利用者a
3
3
利用者b

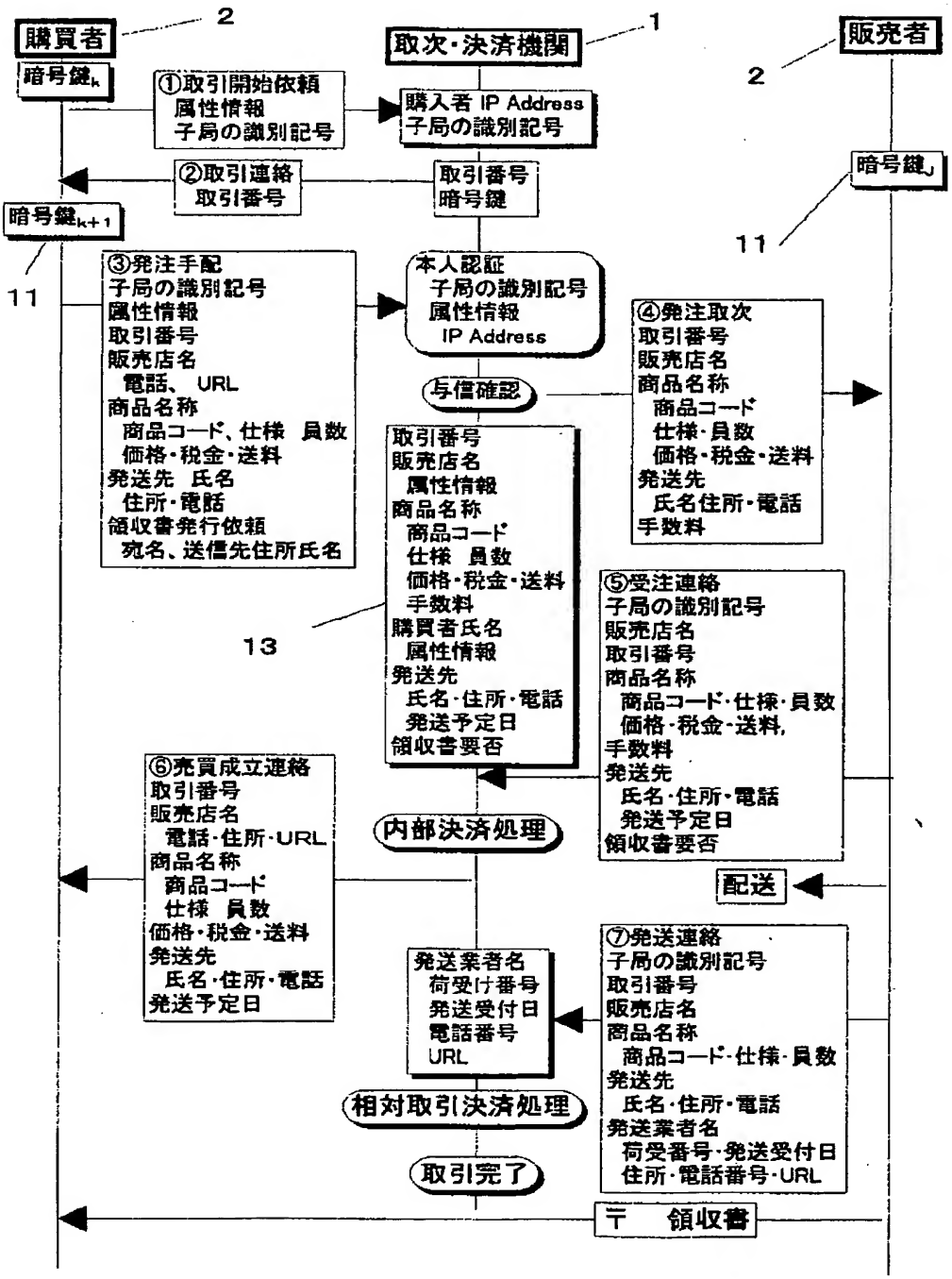
【図１７】


2
子局2₁
子局2₂
… …
子局2ⱼ
18
17
20
18、19
2
インターネット
電話網
その他
1
子局1ᵢ
サーバ
ファイアウォール
22
子局11
子局12
子局13
… …
子局1k
2
利用者
利用者
利用者
利用者
3

【図１８】


1
親局
3
利用者a
共通の暗号鍵もしくは暗号鍵と暗号方式
3
利用者b
利用者c
2
2
子局A
子局C
3
子局B
2
暗号化
復号化
暗号情報
暗号化
復号化
暗号情報
暗号化
復号化
21
21

【図１３】


購買者
2
暗号鍵k
①取引開始依頼
属性情報
子局の識別記号
取次・決済機関
1
購入者 IP Address
子局の識別記号
販売者
2
②取引連絡
取引番号
取引番号
暗号鍵
暗号鍵k+1
11
暗号鍵j
11
③発注手配
子局の識別記号
属性情報
取引番号
販売店名
電話、 URL
商品名称
商品コード、仕様 員数
価格・税金・送料
発送先 氏名
住所・電話
領収書発行依頼
宛名、送信先住所氏名
本人認証
子局の識別記号
属性情報
IP Address
与信確認
④発注取次
取引番号
販売店名
商品名称
商品コード
仕様・員数
価格・税金・送料
発送先
氏名住所・電話
手数料
取引番号
販売店名
属性情報
商品名称
商品コード
仕様 員数
価格・税金・送料
手数料
購買者氏名
属性情報
発送先
氏名・住所・電話
発送予定日
領収書要否
13
⑤受注連絡
子局の識別記号
販売店名
取引番号
商品名称
商品コード・仕様・員数
価格・税金・送料,
手数料
発送先
氏名・住所・電話
発送予定日
領収書要否
⑤売買成立連絡
取引番号
販売店名
電話・住所・URL
商品名称
商品コード
仕様 員数
価格・税金・送料
発送先
氏名・住所・電話
発送予定日
内部決済処理
配送
発送業者名
荷受け番号
発送受付日
電話番号
URL
⑦発送連絡
子局の識別記号
取引番号
販売店名
商品名称
商品コード・仕様・員数
発送先
氏名・住所・電話
発送業者名
荷受番号・発送受付日
住所・電話番号・URL
相対取引決済処理
取引完了
〒 領収書